CITIZEN'S ADVISORY COUNCIL TO LA PORTE INDUSTRY

Plant Security

Houston Ship Channel Security District

Jessica Thomas, Director of Security for the Port Houston Authority and Vice Chairman of the Houston Ship Channel Security District (HSCSD), provided an overview of the District's creation, purpose, and operations. Established on June 9, 2009, by the Harris County Commissioners Court, the HSCSD oversees cost-effective security solutions for the Houston Ship Channel, a critical hub for 250 companies. Leveraging over $30 million in federal Port Security Grants, the District has installed advanced security infrastructure and funded maintenance and operational services. Over the past 13 years, an additional $75.8 million in Port Security Grant projects and assets have been secured, with HSCSD contributing a 25% local cost match.

The Houston Ship Channel Security District is unique in the United States, representing a public-private partnership dedicated to enhancing security for the region's waterside and landside supply chains. Its mission is to improve safety for facilities, employees, and communities within its boundaries by supporting initiatives that strengthen first responders, law enforcement, and regional organizations' capabilities, communication, and operational readiness. Funding is derived from a tax assessment on companies within the ship channel, allocated strictly for regional security enhancements.

Local partnerships include industry partners, the East Harris County Manufacturers Association (EHCMA), Port Houston, Harris County, the cities of Houston and Baytown, the Department of Public Safety (DPS), the United States Coast Guard (USCG), the Department of Homeland Security (DHS), the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Bureau of Investigation (FBI).

Security measures funded by the District include cutting-edge surveillance and detection technology, such as wireless and fiber optic communication systems, night vision, motion detection, radar, sonar, and security sensors. Additional assets include patrol vehicles, SAFE boats, aircraft, and bomb-detection units. The District's board, composed of 11 members representing four zones, works closely with local, state, and federal agencies, as well as industry partners, to address threats such as cyberattacks, terrorism, and insider risks. Mitigation efforts

include cybersecurity measures, background and drug screenings, training programs, and public education initiatives like “See Something, Say Something.”

The HSCSD’s infrastructure and services ensure rapid response times, improved information sharing, and coordinated multi-agency emergency response capabilities, maintaining the Houston Ship Channel as one of the most secure and strategically managed ports in the nation.

Cybersecurity

Dave Bang, Senior Trust Advisor for the LyondellBasell Cybersecurity Program, spoke on cybersecurity. He began his discussion with a cybersecurity safety moment, emphasizing the importance of Multi-Factor Authentication (MFA). MFA enhances security by adding an additional layer of protection, requiring at least two elements—a combination of something you know (such as a password) and something you have (like a phone or security token). He encouraged using MFA whenever possible, noting that most reputable banking, social media, and e-commerce platforms offer it, though it may sometimes be optional or hidden within settings. Bang highlighted that implementing MFA can make systems 99% secure, significantly reducing vulnerability to cyber threats.

Bang outlined LyondellBasell’s Risk Management Framework and program overview, emphasizing its comprehensive approach to cybersecurity. Key components include a standard control framework, workforce education, repeatable processes, defense-in-depth strategies, regular assessments, network monitoring, incident response, risk management, and clearly defined policies and standards. These measures are designed to mitigate threats while assessing and determining the organization’s risk tolerance.

The first step in this process is to decide how much risk a company can handle. LyondellBasell operates with a low-risk tolerance, guided by the principle that cybersecurity risks are only accepted to achieve essential business objectives and with extreme reluctance. The company employs a systematic approach to evaluating and defining risk tolerance, prioritizing the safeguarding of digital assets.

He identified the top cybersecurity threats, with ransomware being the number one concern. Ransomware attacks are becoming more frequent and sophisticated, utilizing new techniques such as generative AI. Additionally, ransomware attacks targeting mobile devices have significantly increased. Other threats include privileged access abuse, where insider neglect or malicious activity targets high-level accounts; supply chain attacks, which often exploit trusted third-party relationships; and dynamic threat surfaces, such as cloud services, generative AI, machine learning, and acquisitions in higher-risk countries.

Bang provided an overview of ransomware, a malware type that locks users out of systems and demands payment. He explained the attack process, from initial intrusion and reconnaissance to data exfiltration, encryption, and ransom demands—often occurring within 15 minutes. To prevent ransomware, he advised downloading security updates promptly, avoiding suspicious emails or websites, and ensuring website authenticity. If targeted, victims should never pay the

ransom but instead, restore systems from backups and report the incident to their company's help desk or, for personal accounts, to the FBI.

James Knox, Business System Security Manager for the LyondellBasell Cybersecurity Program, discussed their Business System Security (BSS) organization, established in 2020 to enhance the focus on information security at sites and within process control networks (PCN). The BSS serves as the primary cybersecurity point of contact for digital technology (DT) and Integrated Process Automation Control (IPAC), fosters strong partnerships with manufacturing, ensures a balance between security and the availability of site OT systems, and closely monitors industry best practices. Note: OT systems, or Operational Technology systems, refer to hardware and software designed to monitor and control physical processes, machinery, and equipment in industrial settings. These systems are critical for ensuring the safety, efficiency, and reliability of operations in sectors such as manufacturing, energy, utilities, transportation, and more.

Knox described the strategies they use to secure their operational technologies. They begin by modeling assets, threats, and risks to identify vulnerabilities and develop mitigation plans. Employees are restricted from accessing the internet on certain systems to reduce exposure to external threats, and regular password updates are enforced to enhance security.

Equipment and software are consistently updated to address vulnerabilities, and critical systems are isolated with additional controls to prevent unauthorized access. The organization employs internal software systems and engages external groups to conduct independent evaluations of their security presence. Simulations are run to test their readiness for various scenarios, and employees are trained on how to respond effectively to potential threats.

Their ultimate goal is to keep the bad guys out, the good data in, and let business do business.

Bang discussed the people side of security awareness and education which includes cybersecurity training, ad-hoc skills development, and in-person training sessions. Employees receive alerts and articles about current events and incidents, and regular skills testing is conducted to assess their ability to recognize phishing and vishing attempts. Phishing is a cyberattack where attackers impersonate legitimate entities to trick individuals into providing sensitive information, such as passwords, credit card numbers, or personal data, typically through fraudulent emails, websites, or messages. Vishing (voice phishing) is a type of cyberattack where attackers use phone calls or voice messages to impersonate legitimate organizations and deceive individuals into revealing sensitive information, such as personal details, passwords, or financial data.

The CAC is a forum for candid and constructive dialogue between those who live or work in La Porte, Morgan’s Point, and Shoreacres and the managers of 41 chemical plants in La Porte. The CAC welcomes visitors. It meets again on Tuesday, February 4 at 6:00 p.m. to learn about flaring. Contact info@laportecac.org if you wish to attend. The CAC shares information about its meetings and presentations at www.laportecac.org.